Groupe de travail Réseau
Request for Comments : 4515
RFC rendues obsolètes : 2254
Catégorie : Norme
Juin 2006

M. Smith, Ed., Pearl Crescent, LLC
T. Howes, Opsware, Inc.
Traduction Claude Brière de L'Isle
décembre 2006

Protocole léger d'accès à un répertoire (LDAP) : Représentation de chaîne des filtres de recherche

Statut de ce mémo

Le présent document spécifie un protocole de normalisation Internet pour la communauté de l'Internet, qui appelle à la discussion et à des suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Normes de protocole officielles de l'Internet" (STD 1) sur l'état de la normalisation et le statut de ce protocole. La distribution du présent mémo n'est soumise à aucune restriction.

Résumé

Les filtres de recherche du protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*) sont transmis dans le protocole LDAP en utilisant une représentation binaire qui est appropriée pour l'utilisation sur le réseau. Le présent document définit une représentation de chaîne lisible par l'homme des filtres de recherche LDAP qui est appropriée pour l'utilisation dans les URL de LDAP (RFC 4516) et dans d'autres applications.

Table des matières

1 Introduction....1
2 Définition de filtre de recherche LDAP....2
3 Définition de filtre de recherche de chaîne....2
4 Exemples....4
5 Considérations sur la sécurité....5
6 Références normatives....5
7 Références informatives....5
8 Remerciements....6
Appendice A Changements depuis la RFC 2254....6

1 Introduction

Le protocole léger d'accès à un répertoire (LDAP) [RFC4510] définit une représentation de réseau de filtre de recherche transmis à un serveur LDAP. Certaines applications peuvent trouver utile d'avoir une façon commune de représenter ces filtres de recherche sous une forme lisible par l'homme ; les URL LDAP [RFC4516] sont un exemple d'une telle application. Le présent document définit un format de chaîne lisible par l'homme pour représenter toute la gamme possible des filtres de recherche LDAP de version 3, y compris les filtres de correspondance étendue.

Le présent document fait partie intégrante de la spécification technique LDAP [RFC4510], qui rend obsolète la spécification technique LDAP précédemment définie, la RFC 3377, dans sa totalité. Le présent document remplace la RFC 2254. Les changements à la RFC 2254 sont résumés à l'Appendice A.

Les mots clé "DOIT", "NE DOIT PAS", "EXIGE", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDÉ", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans le BCP 14 [RFC2119].

2 Définition de filtre de recherche LDAP

Un filtre de recherche LDAP est défini au paragraphe 4.5.1 de la [RFC4511] comme suit :

```
Filter ::= CHOICE {
and             [0] SET SIZE (1..MAX) OF filter Filter,
or              [1] SET SIZE (1..MAX) OF filter Filter,
not             [2] Filter,
equalityMatch   [3] AttributeValueAssertion,
substrings      [4] SubstringFilter,
greaterOrEqual  [5] AttributeValueAssertion,
lessOrEqual     [6] AttributeValueAssertion,
present         [7] AttributeDescription,
approxMatch     [8] AttributeValueAssertion,
extensibleMatch [9] MatchingRuleAssertion }

SubstringFilter ::= SEQUENCE {
type            AttributeDescription, -- initial et final peuvent survenir au plus une fois
substrings      SEQUENCE SIZE (1..MAX) OF substring CHOICE {
initial         [0] AssertionValue,
any             [1] AssertionValue,
final           [2] AssertionValue } }

AttributeValueAssertion ::= SEQUENCE {
attributeDesc   AttributeDescription,
assertionValue  AssertionValue }

MatchingRuleAssertion ::= SEQUENCE {
matchingRule    [1] MatchingRuleId OPTIONAL,
type            [2] AttributeDescription OPTIONAL,
matchValue      [3] AssertionValue,
dnAttributes    [4] BOOLEAN DEFAULT FALSE }

AttributeDescription ::= LDAPString – Restreint à <attributedescription> [RFC4512]

AttributeValue ::= OCTET STRING

MatchingRuleId ::= LDAPString

AssertionValue ::= OCTET STRING

LDAPString ::= OCTET STRING – codé en UTF-8, caractères [Unicode]
```

AttributeDescription, tel que défini dans la [RFC4511], est une représentation de chaîne de la description d'attribut qui est discutée dans la [RFC4512]. Les CHAINES D'OCTET AttributeValue et AssertionValue ont la forme définie dans la [RFC4517]. Le filtre est codé pour les transmissions sur un réseau en utilisant les règles de codage de base (BER, *Basic Encoding Rules*) définies dans la recommandation [X.690], avec les simplifications décrites dans la [RFC4511].

3 Définition de filtre de recherche de chaîne

La représentation de chaîne d'un filtre de recherche LDAP est une chaîne de caractères Unicode [Unicode] codés en UTF-8 [RFC3629] qui est définie par la grammaire suivante, selon la notation ABNF définie dans la [RFC4234]. Les productions utilisées qui ne sont pas définies ici sont définies au paragraphe 1.4 (Productions ABNF communes) de la [RFC4512] sauf mention contraire. Le format de filtre utilise une notation avec un préfixe.

```
filter          = LPAREN filtercomp RPAREN
filtercomp      = and / or / not / item
and             = AMPERSAND filterlist
```

```
or              = VERTBAR filterlist
not             = EXCLAMATION filter
filterlist      = 1*filter
item            = simple / present / substring / extensible
simple          = attr filtertype assertionvalue
filtertype      = equal / approx / greaterorequal / lessorequal
equal           = EQUALS
approx          = TILDE EQUALS
greaterorequal  = RANGLE EQUALS
lessorequal     = LANGLE EQUALS
extensible      = ( attr [dnattrs]
                  [matchingrule] COLON EQUALS assertionvalue )
                  / ( [dnattrs]
                  matchingrule COLON EQUALS assertionvalue )
present         = attr EQUALS ASTERISK
substring       = attr EQUALS [initial] any [final]
initial         = assertionvalue
any             = ASTERISK *(assertionvalue ASTERISK)
final           = assertionvalue
attr            = attributedescription
                  ; La règle attributedescription est définie au paragraphe 2.5 de la [RFC4512].
dnattrs         = COLON "dn"
matchingrule    = COLON oid
assertionvalue  = valueencoding
                  ; La règle <valueencoding> sert à coder une <AssertionValue> du 4.1.6 de la [RFC4511].
valueencoding   = 0*(normal / escaped)
normal          = UTF1SUBSET / UTFMB
escaped         = ESC HEX HEX
UTF1SUBSET      = %x01-27 / %x2B-5B / %x5D-7F
                  ; UTF1SUBSET exclu 0x00 (NUL), LPAREN, RPAREN, ASTERISK, et ESC.
EXCLAMATION     = %x21 ; point d'exclamation ("!")
AMPERSAND       = %x26 ; éperluette (ou symbole ET) ("&")
ASTERISK        = %x2A ; astérisque ("*")
COLON           = %x3A ; point (":")
VERTBAR         = %x7C ; barre verticale ("|")
TILDE           = %x7E ; tilde ("~")
```

Noter que bien que les deux productions <substring> et <present> dans la grammaire ci-dessus puisse produire la construction "attr=*", cette construction n'est utilisée que pour noter un filtre de présence.

La règle <valueencoding> assure que la chaîne de filtre toute entière est une chaîne UTF-8 valide et veille à ce que les octets qui représentent les caractères ASCII "*" (ASCII 0x2a), "(" (ASCII 0x28), ")" (ASCII 0x29), "\" (ASCII 0x5c), et NUL (ASCII 0x00) soient représentés par une barre oblique inversée "\" (ASCII 0x5c) suivie par les deux chiffres hexadécimaux qui représentent la valeur de l'octet codé.

Ce mécanisme d'échappement simple élimine les ambiguïtés d'analyse de filtre et permet à tout filtre qui peut être représenté en LDAP d'être représenté comme une chaîne se terminant par NUL. Les autres octets qui font partie de l'ensemble <normal> peuvent être échappés en utilisant ce mécanisme, par exemple, pour les caractères ASCII non imprimables.

Pour les AssertionValues qui contiennent des données de caractères UTF-8, chaque octet du caractère à échapper est remplacé par une barre oblique inversée et deux chiffres hexadécimaux qui forment un seul octet dans le code du caractère. Par exemple, le filtre vérifiant si l'attribut "cn" contenait une valeur avec le caractère "*" quelque part en son sein serait représenté par "(cn=*\2a*)".

Comme indiqué par la règle <valueencoding>, les mises en œuvre DOIVENT échapper tous les octets supérieurs à 0x7F qui ne font pas validement partie d'une séquence ce codage UTF-8 lorsqu'ils génèrent une représentation de chaîne d'un filtre de recherche. Les mises en œuvre DEVRAIENT accepter en entrée les chaînes qui ne sont pas des chaînes UTF-8 valides. Ceci est nécessaire parce que la RFC 2254 n'a pas clairement défini le terme "représentation de

chaîne" (et en particulier n'a pas mentionné que la représentation de chaîne d'un filtre de recherche LDAP est une chaîne de caractères Unicode codés en UTF-8).

4 Exemples

La présente section donne quelques exemples de filtres de recherche écrits en utilisant cette notation.

```
(cn=Babs Jensen)
(!(cn=Tim Howes))
(&(objectClass=Person)(|(sn=Jensen)(cn=Babs J*)))
(o=univ*of*mich*)
(seeAlso=)
```

Les exemples suivants illustrent l'utilisation de la confrontation extensible.

```
(cn:caseExactMatch:=Fred Flintstone)
(cn:=Betty Rubble)
(sn:dn:2.4.6.8.10:=Barney Rubble)
(o:dn:=Ace Industry)
(:1.2.3:=Wilma Flintstone)
(:DN:2.4.6.8.10:=Dino)
```

Le premier exemple montre l'utilisation de la règle de correspondance "caseExactMatch."

Le second exemple montre l'utilisation d'une forme MatchingRuleAssertion sans matchingRule.

Le troisième exemple illustre l'utilisation de la notation ":oid" pour indiquer que la règle de correspondance identifiée par l'OID "2.4.6.8.10" devrait être utilisée pour faire des comparaisons, et que les attributs du nom distinctif d'une entrée devraient être considérés comme faisant partie de l'entrée lors de l'évaluation de la confrontation (indiquée par l'utilisation de ":dn").

Le quatrième exemple note une confrontation pour égalité, sauf que les composants de nom distinctif devraient être considérés comme faisant partie de l'entrée lorsqu'on effectue la confrontation.

Le cinquième exemple est un filtre qui devrait être appliqué à tout attribut qui prend en charge la règle de correspondance donnée (car le <attr> a été omis).

Le sixième et dernier exemple est aussi un filtre qui devrait s'appliquer à tout attribut qui prend en charge la règle de correspondance donnée. Les attributs qui prennent en charge la règle de correspondance contenue dans le DN devraient aussi être pris en considération.

Les exemples suivants illustrent l'utilisation du mécanisme d'échappement.

```
(o=Parens R Us \28for all your parenthetical needs\29)
(cn=*\2A*)
(filename=C:\5cMyFile)
(bin=\00\00\00\04)
(sn=Lu\c4\8di\c4\87)
(1.3.6.1.4.1.1466.0=\04\02\48\69)
```

Le premier exemple montre l'utilisation du mécanisme d'échappement pour représenter les caractères de parenthèses. Le second montre comment représenter une "*" dans une valeur d'assertion, l'empêchant d'être interprétée comme un indicateur de sous-chaîne. Le troisième illustre l'échappement du caractère barre oblique inversée.

Le quatrième exemple montre un filtre recherchant la valeur de quatre octets 00 00 00 04 (hex), illustrant l'utilisation du mécanisme d'échappement pour représenter des données arbitraires, y compris les caractères NUL.

Le cinquième exemple illustre l'utilisation du mécanisme d'échappement pour représenter divers caractères UTF-8 non ASCII. Précisément, il y a cinq caractères dans la portion <assertionvalue> de cet exemple :

LETTRE LATINE MAJUSCULE L (U+004C), LETTRE LATINE U MINUSCULE (U+0075), LETTRE LATINE C MINUSCULE AVEC CARON (U+010D), LETTRE LATINE I MINUSCULE (U+0069), et LETTRE LATINE C MINUSCULE AVEC ACCENT AIGU (U+0107).

Le sixième et dernier exemple monstre l'assertion d'une valeur codée en BER.

5 Considérations sur la sécurité

Le présent mémo décrit une représentation de chaîne de filtres de recherche LDAP. Bien que la représentation elle-même n'ait pas d'implication connue sur la sécurité, les filtres de recherche LDAP en ont. Ils sont interprétés par les serveurs LDAP pour choisir les entrées à partir desquelles les données sont restituées. Les serveurs LDAP devraient veiller à protéger les données dont ils assurent la maintenance contre les accès non autorisés.

Pour des informations complémentaires, prière de se référer aux sections sur les Considérations sur la sécurité des [RFC4511] et [RFC4513].

6 Références normatives

[RFC2119] Bradner, S., "Mots clé à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[RFC3629] Yergeau, F., "UTF-8, un format de transformation de ISO 10646", STD 63, RFC 3629, novembre 2003.

[RFC4234] Crocker, D. and P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", RFC 4234, octobre 2005.

[RFC4510] Zeilenga, K., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Descriptif des spécifications techniques", RFC 4510, juin 2006.

[RFC4511] Sermersheim, J., Ed., "Protocole léger d'accès à un répertoire (LDAP) Le protocole", RFC 4511, juin 2006.

[RFC4512] Zeilenga, K., "Protocole léger d'accès à un répertoire (LDAP) : Modèle d'informations de répertoires", RFC 4512, juin 2006.

[RFC4513] Harrison, R., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Méthodes d'authentification et mécanismes de sécurité", RFC 4513, juin 2006.

[RFC4517] Legg, S., Ed., "Protocole léger d'accès à un répertoire (LDAP) : Syntaxes et règles de correspondance", RFC 4517, juin 2006.

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3.2.0" *(Norme Unicode, version 3.2.0)* est définie par "The Unicode Standard, Version 3.0" (Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), telle qu'amendée par "Unicode Standard Annex #27: Unicode 3.1" (http://www.unicode.org/reports/tr27/) et par "Unicode Standard Annex #28: Unicode 3.2" (http://www.unicode.org/reports/tr28/).

7 Références informatives

[RFC4516] Smith, M., Ed. et T. Howes, "Protocole léger d'accès à un répertoire (LDAP) : Localisateur universel de ressources", RFC 4516, juin 2006.

[X.690] Union Internationale des Télécommunication – Secteur de la normalisation des télécommunications, "Spécification des règles de codage ASN.1 : Règles de codage de base (BER), Règles de codage canoniques (CER), et Règles de codage distinctives (DER)", X.690(1997) (aussi ISO/IEC 8825-1:1998).

8 Remerciements

Le présent document remplace la RFC 2254 par Tim Howes. La RFC 2254 a été produite par le groupe de travail ASID de l'IETF.

Les changements inclus dans cette spécification révisée se fondent sur des discussions entre les auteurs, des discussions au sein du groupe de travail (ldapbis) de révision de LDAP (v3), et de discussions au sein d'autres groupes de travail de l'IETF. De vifs remerciements vont aux contributions individuelles dans ces groupes de travail.

Appendice A Changements depuis la RFC 2254

A.1 Changements techniques

Remplacement de la référence [ISO 10646] par [Unicode].

Les changements techniques suivants ont été apportés au contenu de la section "Définition du filtre de recherche de chaîne" :

Ajout de la déclaration que la représentation de chaîne est une chaîne de caractères Unicode codés en UTF-8.

Révision de tout l'ABNF pour utiliser les productions communes tirées de la [RFC4512].

Remplacement de la règle "value" par une nouvelle règle "assertionvalue" dans les règles "simple", "extensible", et "substring" ("initial", "any", et "final"). Cela correspond à un changement dans la [RFC4517].

Ajout de "(" et ")" autour des composants des sous productions <extensible> pour précision.

Révision de l'ABNF de "attr", "matchingrule", et "assertionvalue" pour faire plus précisément référence aux productions tirées des documents [RFC4512] et [RFC4511].

Dans la section "Définition de filtre de recherche de chaîne" : remplacé "greater" et "less" par "greaterorequal" et "lessorequal" pour éviter la confusion.

Introduction de "valueencoding" et des règles "normal" et "escaped" associées pou réduire la dépendance au texte descriptif. La production "normal" restreint les chaînes de filtre à des séquences UTF-8 valides.

Ajout d'une déclaration sur le comportement attendu à cause du manque d'une définition claire d'une "représentation de chaîne" dans la RFC 2254.

A.2 Changements rédactionnels

Changement du titre du document pour inclure le préfixe "LDAP:".

Retrait de la note IESG sur le manque de mécanisme d'authentification obligatoire satisfaisant.

Section "Adresse des auteurs" : ajout de Mark Smith comme éditeur du document et mise à jour des informations d'affiliation et de contact.

Ajout des sections "Table des matières" et "Propriété intellectuelle".

Copyright : mise à jour selon les dernières lignes directrices de l'IETF.

Section "Résumé" séparée de l'introduction.

Section "Introduction" nouvelle, séparée du résumé. Mise à jour du second paragraphe pour indiquer que la RFC 2254 est remplacée par le présent document (au lieu de la RFC 1960). Ajout d'une référence à la [RFC4510].

Section "Définition de filtre de recherche de chaîne" : des corrections à l'ABNF de filtre de recherche LDAP de façon qu'il corresponde à celui utilisé dans la [RFC4511].

Précision à la définition de 'value' (maintenant 'assertionvalue') pour tenir compte du fait qu'elle n'est pas précisément une AttributeAssertion d'après le paragraphe 4.1.6 de la [RFC4511] (un traitement particulier est nécessaire pour certains caractères). Ajout d'une note disant que chaque octet d'un caractère à échapper est remplacé par une barre oblique inversée et deux chiffres hexadécimaux, qui représentent un seul octet.

A la section "Exemples" : ajout de quatrr exemples supplémentaires : (seeAlso=), (cn:=Betty Rubble), (:1.2.3:=Wilma Flintstone), et (1.3.6.1.4.1.1466.0=\04\02\48\69). Replacement d'une occurrence de "une valeur" par "une valeur d'assertion". Correction de la description de cet exemple: (sn:dn:2.4.6.8.10:=Barney Rubble). Replacement de l'OID numérique dans le premier exemple de confrontation extensible par "caseExactMatch" pour montrer l'utilisation de la forme descriptive. Utilisation de "DN" (en majuscules) dans le dernier exemple de confrontation extensible pour rappeler au lecteur de traiter les productions <dnattrs> comme insensibles à la casse. Reformulation de la description des quatre exemples de mécanisme d'échappement pour éviter de faire des hypothèses sur l'ordre des octets. Ajout de texte au cinquième exemple de mécanisme d'échappement pour souligner que les caractères non ASCII sont en termes d'Unicode.

A la section "Considérations sur la sécurité" : ajout de références aux [RFC4511] et [RFC4513].

Section "Références normatives" : renommées d'après "Références" selon les nouvelles lignes directrices pour les RFC. Changement du style [1] au style de la [RFC4511] tout au long du document. Ajout d'entrées pour [Unicode], [RFC2119], [RFC4513], [RFC4512], et [RFC4510] et mise à jour de la référence à UTF-8. Remplacement de la référence à la RFC 822 par une référence à la RFC 4234.

Section "Références informatives" : (nouvelle section) déplacement de [X.690] dans cette section. Ajout d'une référence à la [RFC4516].

Ajout de la section "Remerciements".

Ajout de "Appendice A : Changements depuis la RFC 2254".

Entourage des noms de toutes les productions en ABNF par des "<" et ">" lorsqu'elles sont utilisées dans du texte descriptif.

Remplacement de toutes les occurrences de "LDAPv3" par "LDAP."

Adresse des auteurs

Mark Smith, Editor	Tim Howes
Pearl Crescent, LLC	Opsware, Inc.
447 Marlpool Dr.	599 N. Mathilda Ave.
Saline, MI 48176	Sunnyvale, CA 94085
USA	USA
tél : +1 734 944-2856	tél : +1 408 744-7509
mél : mcs@pearlcrescent.com	mél : howes@opsware.com

Déclaration de copyright

L'UTILISATION DES INFORMATIONS CI-ENCLOSES NE VIOLENT AUCUN DROIT OU AUCUNE GARANTIE IMPLICITE DE COMMERCIALISATION OU D'APTITUDE À UN OBJET PARTICULIER.

Propriété intellectuelle

L'IETF ne prend pas position sur la validité et la portée de tout droit de propriété intellectuelle ou autres droits qui pourrait être revendiqués au titre de la mise en œuvre ou l'utilisation de la technologie décrite dans le présent document ou sur la mesure dans laquelle toute licence sur de tels droits pourrait être ou n'être pas disponible o pas plus qu'elle ne prétend avoir accompli aucun effort pour identifier de tels droits. Les informations sur les procédures de l'ISOC au sujet des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif de l'IETF (IASA, *Administrative Support Activity*).